What is claimed is:

1. A method for testing compliance of a target comprising the steps of:

providing a set of regulations;

providing a set of vulnerabilities;

providing a mapping relationship between at least one regulation and at least one vulnerability;

testing a target for a vulnerability in the set of vulnerabilities to determine a vulnerability violation;

associating a regulation in the set of regulations with the vulnerability violation as a function of the mapping to determine a regulation violation.

2. The method of claim 1 wherein the regulations are defined by HIPAA.

3. The method of claim 1 wherein the regulations are defined by GLBA.

4. The method of claim 1 wherein the providing a mapping step further comprises creating a relational database.

5. The method of claim 4 further comprising:

providing a keyword;

scanning the set of regulations by the keyword for a keyed regulation;

scanning the set of vulnerabilities by the keyword for a keyed vulnerability;

grouping the keyed regulation with the keyed vulnerability.

6. The method of claim 1 wherein the testing step further comprises scanning a target to provide a system scan.

7. The method of claim 6 further comprising the step of providing a test set as a function of the system scan.

8. The method of claim 1 further comprising generating a report including an IP address of the target together with the regulation violation.

9. The method of claim 1 further comprising the step of assigning a priority to the regulation violation.

10. The method of claim 1 wherein the set of vulnerabilities are defined by CVE.

11. A security and vulnerability testing system comprising:

a processor;

memory operably connected to the processor;

wherein the memory contains a program executable by the processor to:

search a set of regulations by keyword for a keyed regulation;

search a set of vulnerabilities by the keyword for a keyed vulnerability;

map the keyed regulation to the keyed vulnerability by the keyword to provide a mapping;

test a target for the keyed vulnerability to determine a vulnerability violation;

determine a regulation violation corresponding to the vulnerability violation as a function of the mapping.

12. The system of claim 10 wherein the regulations are defined by HIPAA.

13. The system of claim 10 wherein the regulations are defined by GLBA.

14. The system of claim 10 wherein the set of vulnerabilities are defined by CVE.

15. The system of claim 10 wherein the program is further executable by the processor to scan a target and determine a corresponding test set.

16. The system of claim 10 wherein the program is further executable by the processor to generate a report including an IP address of the target together with the regulation violation.

17. Computer-executable process steps, stored on a computer-readable medium and executable by a processor to perform the steps of:

search a set of regulations by keyword for a keyed regulation;

search a set of vulnerabilities by the keyword for a keyed vulnerability;

map the keyed regulation to the keyed vulnerability to provide a mapping;

test a target for the keyed vulnerability to determine a vulnerability violation;

determine a regulation violation by the keyed vulnerability as a function of the mapping.

18. The steps of claim 17 wherein the regulations are defined by HIPAA.

19. The steps of claim 17 wherein the regulations are defined by GLBA.

20. The steps of claim 17 wherein the set of vulnerabilities are defined by CVE.

21. The steps of claim 17 further executable by the processor to scan a target and determine a corresponding test set.

22. The steps of claim 17 further executable by the processor to generate a report including an IP address of the target together with the regulation violation.

23. The steps of claim 17 further executable by the processor to assign a priority to the regulation violation.